WHAT IS CLAIMED IS:

1. A method comprising:

including data based on at least one of a user identifier and a source identifier in a header of a packet.

2. A method as claimed in claim 1 wherein the data identifying the user identifier is included in a sequence number field of the packet.

3. A method as claimed in claim 1 wherein the data identifying the source identifier is included in an acknowledgement field of the packet.

4. A method as claimed in claim 3 wherein the data in the acknowledgement field has a non-zero value.

5. A method as claimed in claim 1 further comprising:

transforming at least one of the user identifier and source identifier to generate the data for inclusion in the header of the packet.

6. A method as claimed in claim 5 wherein the transforming is performed using a cyclic redundancy check (CRC) algorithm.

7. A method as claimed in claim 5 wherein the data indicating the transformed user identifier is included in a sequence number field of the packet.

8. A method as claimed in claim 7 further comprising:

appending a first key index to the transformed user identifier to generate the data for inclusion in the sequence number field of the packet.

9. A method as claimed in claim 8 wherein the data indicating the transformed source identifier is included in the acknowledgement field of the packet.

10. A method as claimed in claim 9 further comprising:

appending a second key index to the transformed source identifier to form the data for inclusion in the acknowledgement field of the packet.

11. A method as claimed in claim 10 wherein the data included in the acknowledgement field has a non-zero value.

12. A method as claimed in claim 5 further comprising:

appending a key index to the transformed source identifier to generate the data for inclusion in the acknowledgement field of the packet.

13. A method as claimed in claim 1 wherein at least one of the user identifier and source identifier has a non-zero value that is included in the acknowledgement field of the header of the packet.

14. A method as claimed in claim 1 wherein the user identifier indicates a user associated with a source node that initiates communication over a network with a destination node by transmitting the packet from the source node to the destination node.

15. A method as claimed in claim 14 wherein the user identifier comprises a user name of the user.

16. A method as claimed in claim 1 wherein the source identifier indicates a source node that initiates communication over a network with a destination node by transmitting the packet from the source node to the destination node.

17. A method as claimed in claim 16 wherein the source identifier is based on a media access control (MAC) address of the source node.

18. A method as claimed in claim 17 wherein the source node comprises a desktop computer, a laptop computer, personal digital assistant (PDA), or other computing device.

19. A method as claimed in claim 1 wherein the packet has a transfer control protocol / Internet protocol (TCP/IP) format.

20. A method as claimed in claim 1 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

21. A method comprising:

transforming a user identifier;

appending a first key index to the user identifier; and

including the transformed user identifier and appended first key index in a first field of a header of a packet.

22. A method as claimed in claim 21 wherein the user identifier comprises a user name of a user of a node initiating communication with another node using the packet.

23. A method as claimed in claim 21 wherein the user name is subjected to a cyclic redundancy check (CRC) algorithm to generate the transformed user identifier.

24. A method as claimed in claim 21 wherein the node comprises a desktop computer, laptop computer, personal digital assistant (PDA), or other computing device.

25. A method as claimed in claim 21 wherein the packet is a synchronization (SYN) packet.

26. A method as claimed in claim 21 wherein the first field comprises a sequence number field.

27. A method as claimed in claim 21 further comprising:

transforming a source identifier;

appending a second key index to the source identifier; and

including the transformed source identifier and appended second key index in a second field of the packet header.

28. A method as claimed in claim 27 wherein the source identifier identifies a node initiating communication with another node using the packet.

29. A method as claimed in claim 27 wherein the source identifier is a media access control (MAC) address.

30. A method as claimed in claim 29 wherein the node comprises at least one of a desktop computer, laptop computer, personal digital assistant (PDA), or other computing device.

31. A method as claimed in claim 27 wherein the source identifier is subjected to a cyclic redundancy check (CRC) algorithm to generate the transformed source identifier.

32. A method as claimed in claim 27 wherein the packet is a synchronization (SYN) packet.

33. A method as claimed in claim 27 wherein the second field comprises an acknowledgement field.

34. A method as claimed in claim 27 further comprising:

creating a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index;

encrypting the session identifier using a first key identified by the first key index;

generating a hash based on the encrypted session identifier; and

storing at least part of the hash.

35. A method as claimed in claim 34 further comprising:

transmitting the packet including the transformed user identifier and source identifier from the source node at which the transforming is performed, to a destination node.

36. A method as claimed in claim 35 further comprising:

receiving an acknowledgement packet from the destination node in response to the transmitted packet.

37. A method as claimed in claim 36 further comprising:

extracting data from at least one field of the packet;

comparing data from the packet with the hash;

dropping the packet if the extracted data and hash fail to match; and

continuing processing of the packet if the extracted data and the hash match.

38. A method as claimed in claim 37 further comprising:

transmitting the packet including the data indicating the transformed user identifier and source identifier from the source node at which the transforming is performed, to a destination node.

39. A method as claimed in claim 38 further comprising:

receiving an acknowledgement packet from the destination node in response to the transmitted packet.

40. A method as claimed in claim 27 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

41. A method comprising:

generating a packet with a header having a transformed user identifier, a first key index, a transformed session identifier, and a second key index;

creating a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index;

encrypting the session identifier using the first key identified by the first key index; and

generating a hash based on the session identifier; and

storing at least part of the hash.

42. A method as claimed in claim 41 further comprising:

transmitting the packet including the transformed user identifier and source identifier from the source node at which the transforming is performed, to a destination node.

43. A method as claimed in claim 42 further comprising:

receiving an acknowledgement packet from the destination node in response to the transmitted packet.

44. A method as claimed in claim 43 further comprising:

extracting data from the packet;

comparing data from the packet with the hash;

dropping the packet if the extracted data and hash fail to match; and

continuing processing of the packet if the extracted data and the hash match.

45. A method as claimed in claim 41 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

46. A method comprising:

extracting data based on at least one of a user identifier and a source identifier from a header of a packet.

47. A method as claimed in claim 46 wherein the data is extracted from a header of the packet.

48. A method as claimed in claim 46 wherein the packet is a synchronization (SYN) packet.

49. A method as claimed in claim 46 wherein the user identifier is derived from a user name of a user originating the packet.

50. A method as claimed in claim 46 wherein the source identifier is derived from a media access control (MAC) address associated with a node originating the packet.

51. A method as claimed in claim 46 wherein the data includes a transformed user identifier.

52. A method as claimed in claim 51 wherein the transformed user identifier is generated with a cyclic redundancy check (CRC) algorithm.

53. A method as claimed in claim 46 wherein the data includes a transformed source identifier.

54. A method as claimed in claim 53 wherein the transformed source identifier is generated with a cyclic redundancy check (CRC).

55. A method as claimed in claim 46 wherein the data extracted from the packet further comprises at least one key index identifying a key.

56. A method comprising:

receiving a packet having a transformed user identifier, first key index, transformed source identifier, and second key index;

extracting a transformed user identifier, first key index, transformed source identifier, and second key index from a packet;

creating a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index;

encrypting the session identifier using the first key identified by the first key index; and

generating a hash based on the session identifier.

57. A method as claimed in claim 56 wherein the packet is a synchronization (SYN) packet originating from a first node and received at a second node, the method further comprising:

including at least part of the hash for inclusion in a response packet for transmission from the second node to the first node.

58. A method as claimed in claim 57 wherein the part of the hash comprises the lower sixty-four (64) bits of the hash.

59. A method as claimed in claim 56 wherein the user identifier is transformed using a cyclic redundancy check (CRC) algorithm.

60. A method as claimed in claim 56 wherein the encrypting is performed using a DES algorithm.

61. A method as claimed in claim 56 wherein the hash is generated using a SHA-1 algorithm.

62. A method comprising:

receiving a packet;

extracting a user identifier and source identifier from the packet;

checking authorization policy based on the user identifier and source identifier to determine whether the user and source are authorized to pass to a destination indicated by the packet;

releasing the packet if the checking indicates that the packet is permitted by the policy to pass to its destination; and

dropping the packet if the authorization policy indicates that the packet is not permitted to pass to its destination.

63. A method as claimed in claim 62 wherein the packet is a synchronization (SYN) packet.

64. A method as claimed in claim 62 wherein the user identifier is based on a user name of a user of a node originating the packet.

65. A method as claimed in claim 62 wherein the source identifier is based on a media access control (MAC) address of a node originating the packet.

66. A method as claimed in claim 62 wherein the source identifier authorization policy is further defined based on a resource indicated by a destination of the packet.

67. A method as claimed in claim 66 wherein the resource is an application.

68. A method as claimed in claim 66 further comprising:

creating a record of the failed access attempt if the packet is dropped.

69. A method as claimed in claim 66 further comprising:

notifying an administrator of the failed access attempt if the packet is dropped.

70. A method as claimed in claim 66 further comprising:

creating a session identifier based on the transformed user identifier, the first key index, the transformed source identifier, and the second key index;

encrypting the session identifier using the first key identified by the first key index;

generating a hash based on the session identifier;

including the hash in a response packet for transmission to the node originating the received packet; and

transmitting the response packet to the node originating the received packet.

71. A system comprising:

a first node generating a packet including data based on a user identifier and source identifier;

a second node receiving the packet and determining whether the packet is to be released to its destination based on an authorization policy defined for the user identifier and source identifier of the packet; and

a third node receiving and processing the packet if the second node releases the packet to the third node.

72. A system as claimed in claim 71 wherein the packet is a synchronization (SYN) packet defined in transfer control protocol/Internet protocol (TCP/IP) format.

73. A system as claimed in claim 71 wherein at least one of the first, second, and third nodes comprises a desktop computer, laptop computer, personal digital assistant, or other computing device.

74. A system as claimed in claim 71 wherein the first and second nodes are connected via the Internet.

75. A system as claimed in claim 71 wherein the second and third nodes are connected via an intranet.

76. A system as claimed in claim 71 wherein the user identifier is based on a user name of a user of a node originating the packet.

77. A system as claimed in claim 71 wherein the source identifier is based on a media access control (MAC) address of a node originating the packet.

78. A system as claimed in claim 71 wherein the authorization policy is further defined based on a resource indicated by a destination of the packet.

79. A system as claimed in claim 71 wherein the resource is an application.

80. A system as claimed in claim 71 wherein the authorization policy is further defined based on a destination of the packet.

81. A system as claimed in claim 71 further comprising:

creating a record of the failed access attempt if the packet is dropped.

82. A system as claimed in claim 71 further comprising:

notifying an administrator of the failed access attempt if the packet is dropped.

83. An apparatus comprising:

a node for including data based on at least one of a user identifier and a source identifier in a header of a packet.

84. An apparatus as claimed in claim 83 wherein the data identifying the user identifier is included in a sequence number field of the packet.

85. An apparatus as claimed in claim 83 wherein the data identifying the source identifier is included in an acknowledgement field of the packet.

86. An apparatus as claimed in claim 83 wherein the data in the acknowledgement field has a non-zero value.

87. An apparatus as claimed in claim 83 wherein the node transforms at least one of the user identifier and source identifier to generate the data for inclusion in the header of the packet.

88. An apparatus as claimed in claim 87 wherein the node transforms at least one of the user identifier and source identifier using a cyclic redundancy check (CRC) algorithm.

89. An apparatus as claimed in claim 87 wherein the data indicating the transformed user identifier is included in a sequence number field of the packet.

90. An apparatus as claimed in claim 89 wherein the node appends a first key index to the transformed user identifier to generate the data for inclusion in the sequence number field of the packet.

91. An apparatus as claimed in claim 90 wherein the data indicating the transformed source identifier is included in the acknowledgement field of the packet.

92. An apparatus as claimed in claim 91 wherein the node appends a second key index to the transformed source identifier to form the data for inclusion in the acknowledgement field of the packet.

93. An apparatus as claimed in claim 92 wherein the data included in the acknowledgement field has a non-zero value.

94. An apparatus as claimed in claim 87 wherein the node appends a key index to the transformed source identifier to generate the data for inclusion in the acknowledgement field of the packet.

95. An apparatus as claimed in claim 83 wherein at least one of the user identifier and source identifier has a non-zero value that is included in the acknowledgement field of the header of the packet.

96. An apparatus as claimed in claim 83 wherein the user identifier indicates a user associated with a source node that initiates communication over a network with a destination node by transmitting the packet from the source node to the destination node.

97. An apparatus as claimed in claim 96 wherein the user identifier comprises a user name of the user.

98. An apparatus as claimed in claim 83 wherein the node identified by the source identifier is a source node that initiates communication over a network with a destination node by transmitting the packet from the source node to the destination node.

99. An apparatus as claimed in claim 98 wherein the source identifier is based on a media access control (MAC) address of the source node.

100. An apparatus as claimed in claim 98 wherein the source node comprises a desktop computer, a laptop computer, personal digital assistant (PDA), or other computing device.

101. An apparatus as claimed in claim 83 wherein the packet has a transfer control protocol / Internet protocol (TCP/IP) format.

102. An apparatus as claimed in claim 83 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

103. An apparatus comprising:

a node for transforming a user identifier, appending a first key index to the user identifier, and including the transformed user identifier and appended first key index in a first field of a header of a packet.

104. An apparatus as claimed in claim 103 wherein the user identifier comprises a user name of a user of a node initiating communication with another node using the packet.

105. An apparatus as claimed in claim 103 wherein the user name is subjected to a cyclic redundancy check (CRC) algorithm to generate the transformed user identifier.

106. An apparatus as claimed in claim 103 wherein the node comprises a desktop computer, laptop computer, personal digital assistant (PDA), or other computing device.

107. An apparatus as claimed in claim 103 wherein the packet is a synchronization (SYN) packet.

108. An apparatus as claimed in claim 103 wherein the first field comprises a sequence number field.

109. An apparatus as claimed in claim 103 wherein the node further transforms a source identifier, appends a second key index to the source identifier, and includes the transformed source identifier and appended second key index in a second field of the packet header.

110. An apparatus as claimed in claim 109 wherein the source identifier identifies a node initiating communication with another node using the packet.

111. An apparatus as claimed in claim 109 wherein the source identifier is a media access control (MAC) address.

112. An apparatus as claimed in claim 109 wherein the node comprises at least one of a desktop computer, laptop computer, personal digital assistant (PDA), or other computing device.

113. An apparatus as claimed in claim 109 wherein the source identifier is subjected to a cyclic redundancy check (CRC) algorithm to generate the transformed source identifier.

114. An apparatus as claimed in claim 109 wherein the packet is a synchronization (SYN) packet.

115. An apparatus as claimed in claim 109 wherein the second field comprises an acknowledgement field.

116. An apparatus as claimed in claim 109 further comprising:

creating a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index;

encrypting the session identifier using a first key identified by the first key index;

generating a hash based on the encrypted session identifier; and

storing at least part of the hash.

117. A method as claimed in claim 116 further comprising:

transmitting the packet including the transformed user identifier and source identifier from the source node at which the transforming is performed, to a destination node.

118. A method as claimed in claim 117 further comprising:

receiving an acknowledgement packet from the destination node in response to the transmitted packet.

119. A method as claimed in claim 116 further comprising:

extracting data from at least one field of the acknowledgement packet;

comparing data from the acknowledgement packet with the hash;

dropping the acknowledgement packet if the extracted data and hash fail to match; and

continuing processing of the acknowledgement packet if the extracted data and the hash match.

120. A method as claimed in claim 83 further comprising:

transmitting the packet including the data indicating the transformed user identifier and source identifier from the source node at which the transforming is performed, to a destination node.

121. A method as claimed in claim 120 further comprising:

receiving an acknowledgement packet from the destination node in response to the transmitted packet.

122. A method as claimed in claim 83 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

123. An apparatus comprising:

a node for generating a packet with a header having a transformed user identifier, a first key index, a transformed session identifier, and a second key index; creating a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index; encrypting the session identifier using the first key identified by the first key index; generating a hash based on the session identifier; and storing at least part of the hash.

124. An apparatus as claimed in claim 123 wherein the node further transmits the packet including the transformed user identifier and source identifier from the source node at which the transforming is performed, to a destination node.

125. An apparatus as claimed in claim 124 wherein the node further receives an acknowledgement packet from the destination node in response to the transmitted packet.

126. A method as claimed in claim 123 wherein the node further extracts data from the packet, compares data from the packet with the hash, drops the packet if the extracted data and hash fail to match, and continues processing of the packet if the extracted data and the hash match.

127. A method as claimed in claim 123 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

128. An apparatus comprising:

a node for extracting data based on at least one of a user identifier and a source identifier from a header of a packet.

129. An apparatus as claimed in claim 128 wherein the data is extracted from a header of the packet.

130. An apparatus as claimed in claim 128 wherein the packet is a synchronization (SYN) packet.

131. An apparatus as claimed in claim 128 wherein the user identifier is derived from a user name of a user originating the packet.

132. An apparatus as claimed in claim 128 wherein the source identifier is derived from a media access control (MAC) address associated with a node originating the packet.

133. An apparatus as claimed in claim 128 wherein the data includes a transformed user identifier.

134. An apparatus as claimed in claim 133 wherein the transformed user identifier is generated with a cyclic redundancy check (CRC) algorithm.

135. An apparatus as claimed in claim 128 wherein the data includes a transformed source identifier.

136. An apparatus as claimed in claim 135 wherein the transformed source identifier is generated with a cyclic redundancy check (CRC) algorithm.

137. An apparatus as claimed in claim 128 wherein the data extracted from the packet further comprises at least one key index identifying a key.

138. An apparatus comprising:

a node for receiving a packet having a transformed user identifier, first key index, transformed source identifier, and second key index; extracting a transformed user identifier, first key index, transformed source identifier, and second key index from a packet; creating a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index; encrypting the session identifier using the first key identified by the first key index; and generating a hash based on the session identifier.

139. An apparatus as claimed in claim 138 wherein the packet is a synchronization (SYN) packet originating from a first node and received at a second node, the node further including at least part of the hash for inclusion in a response packet for transmission from the second node to the first node.

140 An apparatus as claimed in claim 138 wherein the part of the hash comprises the lower sixty-four (64) bits of the hash.

141. A method as claimed in claim 138 wherein the user identifier is transformed using a cyclic redundancy check (CRC) algorithm.

142. A method as claimed in claim 138 wherein the encrypting is performed using a DES algorithm.

143. A method as claimed in claim 138 wherein the hash is generated using a SHA-1 algorithm.

144. An apparatus comprising:

a node for receiving a packet; extracting a user identifier and source identifier from the packet; checking authorization policy based on the user identifier and source identifier to determine whether the user and source are authorized to pass to a destination indicated by the packet; releasing the packet if the checking indicates that the packet is permitted by the policy to pass to its destination; and dropping the packet if the authorization policy indicates that the packet is not permitted to pass to its destination.

145. A node as claimed in claim 144 wherein the packet is a synchronization (SYN) packet.

146. A node as claimed in claim 144 wherein the user identifier is based on a user name of a user of a node originating the packet.

147. A node as claimed in claim 144 wherein the source identifier is based on a media access control (MAC) address of a node originating the packet.

148. A node as claimed in claim 144 wherein the source identifier authorization policy is further defined based on a resource indicated by a destination of the packet.

149. A node as claimed in claim 144 wherein the resource is an application.

150. A node as claimed in claim 144 wherein the node creates a record of the failed access attempt if the packet is dropped.

151. A node as claimed in claim 144 wherein the node notifies an administrator of the failed access attempt if the packet is dropped.

152. A node as claimed in claim 144 wherein the node creates a session identifier based on the transformed user identifier, the first key index, the transformed source identifier, and the second key index; encrypts the session identifier using the first key identified by the first key index; generates a hash based on the session identifier; includes the hash in a response packet for transmission to the node originating the received packet; and transmits the response packet to the node originating the received packet.

153. A computer-readable medium having a computer program executable by a computing device to include data based on at least one of a user identifier and a source identifier in a header of a packet.

154. A computer-readable medium as claimed in claim 153 wherein the computer program is executable by the computing device to include the data identifying the user identifier in a sequence number field of the packet.

155. A computer-readable medium as claimed in claim 153 wherein the computer program is executable by the computing device to include the data identifying the source identifier in an acknowledgement field of the packet.

156. A computer-readable medium as claimed in claim 153 wherein the computer program is executable by the computing device to generate the data in the acknowledgement field with a non-zero value.

157. A computer-readable medium as claimed in claim 153 wherein the computer program is executable by the computing device to transform at least one of the user identifier and source identifier to generate the data for inclusion in the header of the packet.

158. A computer-readable medium as claimed in claim 153 wherein the computer program is executable by the computing device to transform the user identifier using a cyclic redundancy check (CRC) algorithm.

159. A computer-readable medium as claimed in claim 153 wherein the computer program is executable by the computing device to include the transformed user identifier in a sequence number field of the packet.

160. A computer-readable medium as claimed in claim 159 wherein the computer program is executable by the computing device to append a first key index to the transformed user identifier to generate the data for inclusion in the sequence number field of the packet.

161. A computer-readable medium as claimed in claim 160 wherein the computer program is executable by the computing device to include the data indicating the transformed source identifier in the acknowledgement field of the packet.

162. A computer-readable medium as claimed in claim 161 wherein the computer program is executable by the computing device to append a second key index to the transformed source identifier to form the data for inclusion in the acknowledgement field of the packet.

163. A computer-readable medium as claimed in claim 162 wherein the computer program is executable by the computing device to generate the data included in the acknowledgement field with a non-zero value.

164. A computer-readable medium as claimed in claim 163 wherein the computer program is executable by the computing device to append a key index to the transformed source identifier to generate the data for inclusion in the acknowledgement field of the packet.

165. A computer-readable medium as claimed in claim 153 wherein the computer program is executable by the computing device to generate at least one of the user identifier and source identifier with a non-zero value that is included in the acknowledgement field of the header of the packet.

166. A computer-readable medium as claimed in claim 153 wherein the user identifier indicates a user associated with a source node comprising the computing device, that initiates communication over a network with a destination node by transmitting the packet from the source node to the destination node.

167. A computer-readable medium as claimed in claim 166 wherein the user identifier comprises a user name of the user.

168. A computer-readable medium as claimed in claim 166 wherein the source identifier indicates a source node that initiates communication over a network with a destination node by transmitting the packet from the source node to the destination node.

169. A computer-readable medium as claimed in claim 166 wherein the source identifier is based on a media access control (MAC) address of the source node.

170. A computer-readable medium as claimed in claim 166 wherein the source node comprises a desktop computer, a laptop computer, personal digital assistant (PDA), or other computing device.

171. A computer-readable medium as claimed in claim 153 wherein the packet has a transfer control protocol / Internet protocol (TCP/IP) format.

172. A computer-readable medium as claimed in claim 153 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

173. A computer-readable medium having a computer program for transforming a user identifier; appending a first key index to the user identifier; and including the transformed user identifier and appended first key index in a first field of a header of a packet.

174. A computer-readable medium as claimed in claim 173 wherein the user identifier comprises a user name of a user of a node initiating communication with another node using the packet.

175. A computer-readable medium as claimed in claim 173 wherein the user name is subjected to a cyclic redundancy check (CRC) algorithm to generate the transformed user identifier.

176. A computer-readable medium as claimed in claim 173 wherein the computer program is executed by a node comprising a desktop computer, laptop computer, personal digital assistant (PDA), or other computing device.

177. A computer-readable medium as claimed in claim 173 wherein the packet is a synchronization (SYN) packet.

178. A computer-readable medium as claimed in claim 173 wherein the first field comprises a sequence number field.

179. A computer-readable medium as claimed in claim 173 wherein the computer program is executable by a computing device to transform a source identifier; append a second key index to the source identifier; and include the transformed source identifier and appended second key index in a second field of the packet header.

180. A computer-readable medium as claimed in claim 179 wherein the source identifier identifies a node initiating communication with another node using the packet.

181. A computer-readable medium as claimed in claim 179 wherein the source identifier comprises a media access control (MAC) address.

182. A computer-readable medium as claimed in claim 179 wherein the computer program is executed by a node comprising at least one of a desktop computer, laptop computer, personal digital assistant (PDA), or other computing device.

183. A computer-readable medium as claimed in claim 179 wherein the source identifier is subjected to a cyclic redundancy check (CRC) algorithm to generate the transformed source identifier.

184. A computer-readable medium as claimed in claim 179 wherein the packet is a synchronization (SYN) packet.

185. A computer-readable medium as claimed in claim 179 wherein the second field comprises an acknowledgement field.

186. A computer-readable medium as claimed in claim 179 wherein the computer program can further be executed to create a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index; encrypt the session identifier using a first key identified by the first key index; generate a hash based on the encrypted session identifier; and store at least part of the hash.

187. A computer-readable medium as claimed in claim 179 wherein the computer program can further be executed to transmit the packet including the transformed user identifier and source identifier from the source node at which the transforming is performed, to a destination node.

188. A computer-readable medium as claimed in claim 179 wherein the computer program can further be executed to receive an acknowledgement packet from the destination node in response to the transmitted packet.

189. A computer-readable medium as claimed in claim 173 wherein the computer program can further be executed by the computing device to extract data from at least one field of the packet; compare data from the packet with the hash; drop the packet if the extracted data and hash fail to match; and continue processing of the packet if the extracted data and the hash match.

190. A computer-readable medium as claimed in claim 173 wherein the computer program can be executed by the computing device to transmit the packet including the data indicating the transformed user identifier and source identifier from the source node at which the transforming is performed, to a destination node.

191. A computer-readable medium as claimed in claim 173 wherein the computer program can be executed by the computing device to receive an acknowledgement packet from the destination node in response to the transmitted packet.

192. A computer-readable medium as claimed in claim 173 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

193. A computer-readable medium having a computer program executable by a computing device to generate a packet with a header having a transformed user identifier, a first key index, a transformed session identifier, and a second key index; create a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index; encrypt the session identifier using the first key identified by the first key index; generate a hash based on the session identifier; and store at least part of the hash.

194. A computer-readable medium as claimed in claim 193 wherein the computer program can be executed by the computing device to transmit the packet including the transformed user identifier and source identifier from a source node comprising the computing device at which the transforming is performed, to a destination node.

195. A computer-readable medium as claimed in claim 194 wherein the computer program can be executed by the computing device to receive an acknowledgement packet from the destination node in response to the transmitted packet.

196. A computer-readable medium as claimed in claim 193 wherein the computer program can be executed by the computing device to extract data from the packet, compare data from the packet with the hash, drop the packet if the extracted data and hash fail to match, and continue processing of the packet if the extracted data and the hash match.

197. A computer-readable medium as claimed in claim 193 wherein the packet is a synchronization (SYN) packet used to initiate communication between source and destination nodes in transfer control protocol / Internet protocol (TCP/IP).

198. A computer-readable medium having a computer program for extracting data based on at least one of a user identifier and a source identifier from a packet.

199. A computer-readable medium as claimed in claim 198 wherein the data is extracted from a header of the packet.

200. A computer-readable medium as claimed in claim 198 wherein the packet is a synchronization (SYN) packet.

201. A computer-readable medium as claimed in claim 198 wherein the user identifier is derived from a user name of a user originating the packet.

202. A computer-readable medium as claimed in claim 198 wherein the source identifier is derived from a media access control (MAC) address associated with a node originating the packet.

203. A computer-readable medium as claimed in claim 198 wherein the data includes a transformed user identifier.

204. A computer-readable medium as claimed in claim 203 wherein the transformed user identifier is generated with a cyclic redundancy check (CRC) algorithm.

205. A computer-readable medium as claimed in claim 198 wherein the data includes a transformed source identifier.

206. A computer-readable medium as claimed in claim 205 wherein the transformed source identifier is generated with a cyclic redundancy check (CRC).

207. A computer-readable medium as claimed in claim 198 wherein the data extracted from the packet further comprises at least one key index identifying a key.

208. A computer-readable medium having a computer program executable by a computing device to receive a packet having a transformed user identifier, first key index, transformed source identifier, and second key index; extract a transformed user identifier, first key index, transformed source identifier, and second key index from a packet; create a session identifier based on the transformed user identifier, the first key index, the transformed session identifier, and the second key index; encrypt the session identifier using the first key identified by the first key index; and generate a hash based on the session identifier.

209. A computer-readable medium as claimed in claim 208 wherein the packet is a synchronization (SYN) packet originating from the computing device of a first node, and received at a computing device of a second node, and the computer program is further executable by the computing device of the second node to include at least part of the hash in a response packet for transmission from the second node to the first node.

210. A computer-readable medium as claimed in claim 208 wherein the part of the hash comprises the lower sixty-four (64) bits of the hash.

211. A computer-readable medium as claimed in claim 208 wherein the user identifier is transformed using a cyclic redundancy check (CRC) algorithm.

212. A computer-readable medium as claimed in claim 208 wherein the encrypting is performed using a DES algorithm.

213. A computer-readable medium as claimed in claim 208 wherein the hash is generated using a SHA-1 algorithm.

214. A computer-readable medium having a computer program executable by a node to receive a packet; extract a user identifier and source identifier from the packet; check authorization policy based on the user identifier and source identifier to determine whether the user and source are authorized to pass to a destination indicated by the packet; release the packet if the checking indicates that the packet is permitted by the policy to pass to its destination; and drop the packet if the authorization policy indicates that the packet is not permitted to pass to its destination.

215. A computer-readable medium as claimed in claim 214 wherein the packet is a synchronization (SYN) packet.

216. A computer-readable medium as claimed in claim 214 wherein the user identifier is based on a user name of a user of the node originating the packet.

217. A computer-readable medium as claimed in claim 214 wherein the source identifier is based on a media access control (MAC) address of the node originating the packet.

218. A computer-readable medium as claimed in claim 214 wherein the source identifier authorization policy is further defined based on a resource indicated by a destination of the packet.

219. A computer-readable medium as claimed in claim 214 wherein the resource is an application.

220. A computer-readable medium as claimed in claim 214 wherein the computer program can be executed to create a record of the failed access attempt if the packet is dropped.

221. A computer-readable medium as claimed in claim 214 wherein the computer program can be executed to notify an administrator of the failed access attempt if the packet is dropped.

222. A computer-readable medium as claimed in claim 214 wherein the computer program can be executed to create a session identifier based on the transformed user identifier, the first key index, the transformed source identifier, and the second key index; encrypt the session identifier using the first key identified by the first key index; generate a hash based on the session identifier; include the hash in a response packet for transmission to the node originating the received packet; and transmit the response packet to the node originating the received packet.